

REMARKS

Applicants respectfully traverse and request reconsideration.

Applicants wish to thank the Examiner for the notice that Claims 5-9, 12-17, 19-22, 29-31, 34, 35, 38, 39 and 44-47 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Applicants delete Claim 34 without prejudice.

Claims 1-4, 10, 18, 23, 24, 27, 28, 32, 33, 36, 37, and 40-43 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,481,613 (Ford et al). Ford et al is directed to a computer network cryptographic key distribution system that employs a single key package referred to as an ACD allowing an encryptor to encrypt a message encryption key using a public key of a key release agent, thereby forming the ACD. The encrypted message and ACD, which is a single key package, is sent by an encryptor to a decryptor. The decryptor adds decryptor attributes and then forwards the single key package to the key release agent. The key release agent recovers the messaged decryption key and supplies it back to the decryptor through a protected key release transaction. The key release agent recovers the ACD keys and returns the plain text ACD keys to the decryptor. The decryptor uses the plain text message encryption key and the ACD keys to decrypt the cipher text and obtain plain text. (See Column 7, Lines 63-67). As taught by Ford et al., “the key release transaction must be conducted using protected requests and release messages 44. In particular, the request 34 must be protected by communication, authentication and integrity mechanisms ... and the response 46 must be protected by a communication confidentiality mechanism.” Column 6, Line 66 to Column 7, Line 5. Hence, the plain text ACD keys may later be encrypted using the public key of the decryptor by the KRA (See Column 7, Lin 7). As such Ford et al. teaches that a single key package is sent to a key release agent as forwarded by a decryptor. The key release agent then decrypts the ACD


using its private key and sends the plain text message encryption key back to the encryptor through a protected key release transaction. As such, the key release agent is used to encrypt the message key to effect a protected key release transaction.

Applicants claim a distinctly different approach. Applicants claim, among other things, providing, by the first party, “a double key package.” The double key package is the message encryption key encrypted using a second party public key which is then encrypted using the public key of the third party. In contrast, the encryptor in Ford does not encrypt the ACD using the public key of the decryptor. There does not appear to be a teaching of a double key package as required by the claims. As such, these claims are in condition for allowance. In addition, Claim 10 adds additional novel and non-obvious subject matter where the third party receives back from the second party the double key package. There is no such teaching or suggestion in the Ford et al. reference. Accordingly, these claims are also in condition for allowance.

Claims 11, 25, 26, and 31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Ford et al. in view of Perlman. Applicants respectfully reassert the relevant remarks made above and notes that neither Perlman nor Ford et al. describe the communication and use of a double key package in the way required in the claims. As such, these claims are also believed to be in condition for allowance.

Accordingly, Applicants respectfully submit that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

By: 
Christopher J. Reckamp
Registration No. 34,414

Date: July 14, 2003

Vedder, Price, Kaufman & Kammholz, P.C.
222 N. LaSalle Street
Chicago, IL 60601
PHONE: (312) 609-7500
FAX: (312) 609-5005